AUF (Agence Universitaire pour la Francophonie) Septembre/octobre 2005
Coopération Mathématique inter-universitaire Cambodge France *Michel Waldschmidt*

Master Training Program : Royal Academy of Cambodia/CIMPA

Examen écrit: `21 octobre 2005`

Durée: 3 heures
Aucun document n'est autorisé, aucune calculette non plus

Toutes les réponses doivent être justifiées.

1.
a) Peut-il exister trois ensembles E, F, G et deux applications

$$f : E \to F, \qquad g : F \to G$$

telles que f ne soit pas injective, g ne soit pas surjective et $g \circ f : E \to G$ soit bijective?
b) Peut-il exister trois ensembles E, F, G et deux applications

$$f : E \to F, \qquad g : F \to G$$

telles que f ne soit pas surjective, g ne soit pas injective et $g \circ f : E \to G$ soit bijective?
Pour chacune des deux questions, si votre réponse est non, le démontrer; si votre réponse est oui, donner un exemple.

2. Parmi les nombres ci-dessous (écrits dans le système décimal), dire quels sont ceux qui sont rationnels et donner leur écriture sous forme irréductible a/b avec a et b premiers entre eux, $b > 0$:

$$0.123123123123123\ldots,$$
$$0.1999999999999\ldots$$
$$0.101001000100001000001000000100000001\ldots,$$

`Indication:` dans le dernier développement, les suites de 0 consécutifs ont successivement 1, 2, 3, 4, ... termes.

3. Combien le nombre 86 400 000 a-t-il de diviseurs?

4. Parmi les entiers n satisfaisant $1 \leq n \leq 10\,000$, combien y en a-t-il
a) qui sont premiers avec 10 000?
b) qui sont premiers avec 21?

5.
a) Quel est le pgcd (plus grand commun diviseur) d_1 des deux nombres 2^{360} et 2^{240}?
b) Quel est le pgcd d_2 des deux nombres $2^{360}-1$ et $2^{240}-1$?
c) Quel est le pgcd d_3 des deux nombres $2^{360}-1$ et 2^{240} ?
d) Pour chacun de ces trois nombres d_1, d_2, d_3,
– dire combien il a de chiffres binaires (= en base 2)
– dire approximativement combien il a de chiffres décimaux, en utilisant le fait que le nombre $2^{10}=1024$ est proche de 10^3
– dire quel est le dernier chiffre décimal.

6. Pour chacun des quatre nombres premiers 37, 41, 43, 47, dire
– si 1 est résidu quadratique,
– si -1 est résidu quadratique,
– si 2 est résidu quadratique,
– si -2 est résidu quadratique,
– si 3 est résidu quadratique,
– si 4 est résidu quadratique.

7. On considère un corps fini ayant 64 éléments.
a) Quelle est la caractéristique de ce corps?
b) Quels sont les entiers $n \geq 1$ pour lesquels il existe au moins une racine primitive n-ième de l'unité dans ce corps?
Pour chacune de ces valeurs de n, dire combien il y a de racines primitives n-ièmes de l'unité dans ce corps.

8. Quels sont les générateurs du groupe cyclique $(\mathbf{Z}/7\mathbf{Z})^\times$?
Quels sont les nombres premiers p tels que le polynôme cyclotomique $\Phi_7(X)$ soit irréductible sur le corps fini $\mathbf{F}_p$ à p éléments?

9. Soient $f \in \mathbf{F}_p[X]$ un polynôme irréductible de degré d sur le corps fini $\mathbf{F}_p$ à p éléments, K un corps fini de caractéristique p et $\alpha \in K$ une racine de f. Donner la liste des racines de f dans K.

10. Donner la liste des éléments du code cyclique de longueur 7 sur le corps $\mathbf{F}_2$ à deux éléments dont le polynôme générateur est $1+X+X^2+X^3+X^4+X^5+X^6$.

11. Soit n un entier ≥ 2. On note F_n le nombre de Fermat $2^{2^n}+1$. Soit p un diviseur premier de F_n.
a) Quel est l'ordre de 2 modulo p ?
b) En déduire que p est congru à 1 modulo 2^{n+1}.
c) Le nombre 2 est-il résidu quadratique modulo p ?
d) Montrer que p est congru à 1 modulo 2^{n+2}.

`Le corrigé sera disponible sur le site`
http://www.math.jussieu.fr/~miw/enseignement.html